# APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. 60258-306460

Invention: DETECTING AND BLOCKING MALICIOUS CONNECTIONS

Inventor (s): Joona AIRAMO

**Address communications to the correspondence address associated with our Customer No**

00909

Pillsbury Winthrop LLP

This is a:

- ☐ Provisional Application
- ☒ Regular Utility Application
- ☐ Continuing Application
  - ☐ The contents of the parent are incorporated by reference
- ☐ PCT National Phase Application
- ☐ Design Application
- ☐ Reissue Application
- ☐ Plant Application
- ☐ Substitute Specification
  Sub. Spec Filed _____
  in App. No. _____ / _____
- ☐ Marked up Specification re
  Sub. Spec. filed _____
  In App. No _____ / _____

## SPECIFICATION

# DETECTING AND BLOCKING MALICIOUS CONNECTIONS

## FIELD OF THE INVENTION

**[0001]** The present invention relates to information security and especially to securing a device having data communication capability.

## BACKGROUND OF THE INVENTION

**[0002]** In data networks such as Internet, it is in practice mandatory to have information security measures in place in order to secure proprietary information and to defend against malicious intruders.

**[0003]** An applet is a little application. On the Web (WWW, World Wide Web), using Java, the object-oriented programming language, an applet is a small program that can be sent from a Web server along with a Web page to a user. Java applets can perform interactive animations, immediate calculations, or other simple tasks without having to send a user request back to the server. When a browser requests a Web page with applets, the applets are sent automatically and can be executed as soon as the page arrives in the browser. If the applet is allowed unlimited access to memory and system resources, it can do harm in the hands of someone with malicious intent. For the sake of security, applets are run in "a sandbox", where the applet has only limited access to system resources. The sandbox creates an environment in which there are strict limitations on what system resources the applet can request or access. Sandboxes are used when executable code comes from unknown or untrusted sources and allow the user to run untrusted code safely. However, not all functionality of an applet can be denied even in sandbox. For example, an applet may need to open new outward connections towards the server they originated from.

**[0004]** FTP is an example of commonly used transfer protocols, which consist of more than one separate connection. In such protocols, a first connection is opened and then at least one other connection is opened on the basis of information obtained from or transferred within the first connection. That is, some attributes, such as port numbers, of the other connection are negotiated within the first connection. These are herein referred to as a control connection (the first connection) and a related connection (the other connection). In FTP, the related connection is often called data connection. Such a related connection is always related to some control connection and does not exist alone in a sense that opening the related connection requires interven-

tion of the control connection. In addition, one related connection may be a control connection of another related connection. This concerns for example H.323 protocol. In these protocols, the attributes of related connections usually change dynamically. For example it is usually not known beforehand to which port a related connection will be established. Also the direction in which a related connection is opened may vary.

**[0005]** A firewall is traditionally considered as a set of components forming a gateway between two or more networks, which have different security requirements. Thus, a firewall is a gateway which operates at the same time as a connector and a separator between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. A firewall can be also so called personal firewall, which sits in an individual device, which needs to be protected, and monitors only connections going in to or coming out from that device. The operation of such personal firewall is in principle similar to the operation of a gateway firewall.

**[0006]** A firewall is configured by means of rules, which define which data packets are allowed to traverse the firewall and which are not. A rule comprises information for identifying a data packet (e.g. source and destination addresses and ports) and an associated action, which may be for example to allow or deny the packet. A firewall may be a simple packet filter, which compares header fields of a data packet to the firewall rules and processes the data packet according to the rule, which matches the data packet. A more advanced, stateful, firewall keeps track also on the state of different connections.

**[0007]** In a stateful firewall for example an FTP data connection is allowed only if negotiation of such data connection is noticed within a legitimate control connection. Other protocols comprising of more than one connection are treated similarly to FTP connections in stateful firewalls.

**[0008]** The use of protocols, which open related connections, creates vulnerability in a device, which is running applets, irrespective of whether a firewall is protecting the device or not. Let consider following scenario for illustrating this:

**[0009]** - A Java applet is delivered to a client browser,

**[0010]** - The Java applet acts as an FTP client and opens a control connection to the server,

**[0011]** - A data connection from the server to the client is negotiated for a port in which some other vulnerable service is running (previous experimentation or even an educated guess can be used for finding out such port),

**[0012]** - for an outside process, the data connection seems perfectly legitimate, since it was negotiated within a legitimate control connection, and thus it is allowed to traverse any firewall, either gateway or personal.

**[0013]** Thus the server is allowed to open a connection to a port, where a vulnerable service is running. In some cases connections to ports below 1024 are denied in a firewall, but plenty of vulnerable services can be found also in ports above 1024.

**[0014]** One solution for tackling this vulnerability is to block all related connections. The disadvantage of this solution is that it blocks also all legitimate use of some important protocols. In many cases this is not a viable solution. In case of FTP blocking active FTP would help, but then not even legitimate active FTP connections would be allowed and still related connections associated with other protocols could be exploited. (FTP connections are classified into passive and active; in passive FTP the data connection is opened to the same direction with the control connection and in active FTP the data connection is opened to the opposite direction with the control connection.)Another partial solution would be to monitor related connections and allow them only if data is going only in one direction. This would make malicious use of FTP more complex, since in legitimate FTP data connections data is going only in one direction, but it would not help in relation to protocols in which data is transferred bi-directionally in the related connections. And even FTP attacks would not be disabled by this solution, since past experience has proven that it is possible to craft an attack, which transmits data only to the target and does not require any return traffic.

**[0015]** Thus, a new solution for tackling this problem is needed.

## SUMMARY OF THE INVENTION

**[0016]** An object of the invention is to provide a new solution for securing a device having data communication capability and to mitigate the vulnerability discussed above.

**[0017]** This object of the invention is achieved according to the invention as disclosed in the attached independent claims. Preferred embodiments of the invention are disclosed in the dependent claims. The features described in one dependent claim may be further combined with features described in another dependent claim to produce further embodiments of the invention.

**[0018]** Malicious related connections are detected and blocked by examining relationship between a port negotiated for a related connection and the associated control connection and by deciding on the basis on this relationship, whether the related connection shall be allowed. This relationship may concern for example time elapsed between noticing negotiation of the related connection and opening the associated port. Alternatively the relationship may concern the process, which initiated the control connection, and the process, which opened the port. Also other determinants of the relationship may be used according to the invention. Viable determinants may be such that they indicate reasonably reliably legitimate use of related connections. In this way, opening a malicious related connection to a port, which is used e.g. by some vulnerable service, is prevented in most cases.

**[0019]** According to the invention the method of securing a device having data communication capability comprises

**[0020]** - dynamically detecting a control connection, which originates from said device,

**[0021]** - noticing negotiation of a related connection within said control connection, said negotiation comprising at least defining a port of the device for said related connection,

**[0022]** - checking if relationship between said port of the device and the control connection fulfills predefined criteria, and

**[0023]** - conditionally blocking said related connection, if said port of the device does not fulfill said predefined criteria.

**[0024]** According to an embodiment of the invention said predefined criteria requires that said port of the device is opened within a predefined time

window in relation to noticing negotiation of a related connection within said control connection.

**[0025]** According to another embodiment of the invention said predefined criteria requires that said control connection and said port of the device are opened by the same process family.

**[0026]** The advantage of the invention is that it substantially decreases the vulnerability related to applets discussed above.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0027]** Various features of the invention, as well as the advantages offered thereby, are described hereinafter in more detail with reference to embodiments and aspect of the invention illustrated in the accompanying drawings, in which

**[0028]** Figure 1 illustrates an example network configuration,

**[0029]** Figure 2A is a flow chart illustrating an example of the method of the invention, and

**[0030]** Figure 2B is a flow chart illustrating another example of the method of the invention.

## PREFERRED EMBODIMENTS OF THE INVENTION

**[0031]** Figure 1 illustrates a simplified example network scenario, wherein the invention may be used. Therein a client device 101 is connected to the Internet 102 via a gateway firewall 100. The client device comprises some security measure, which is used for monitoring data going in to and out from the device and which implements functionality of the invention. Such security measure may be for example a personal firewall. A server 103, which provides www-services, is also connected to the Internet 102. The client device 101 may now connect to the server 103 via the gateway firewall 100 and request for a www-page containing an applet. The applet is conveyed to the client device 101 along with the requested www-page, and the applet is automatically run in the client device. (That is, if applets are allowed in the client device.) The applet may open a new connection to the server without security measures intervening in that. Also legitimate related connections can be opened to or from the client device. The gateway firewall 100 does not have means to detect a difference between a malicious related connection and a legitimate one, if there is an associated control connection, which seems to be

legitimate. The only way to block malicious related connections in a gateway firewall or in a traditional personal firewall would be to block all related connections towards the client device 101. But the functionality of the invention included in the client device 101 prevents opening malicious or suspicious related connections to the client and at the same time allows legitimate related connections to the client.

**[0032]** The invention can be employed in any device, which needs to be protected from malicious use of related connections. Physically the device is a computer hardware device combined with appropriate software to do the tasks assigned to it. Examples of such devices are desktop and laptop computers, PDAs (Personal Digital Assistant), mobile phones and smart phones.

**[0033]** One logical place, where to implement the invention, is a personal firewall program, which is running in the client device and which monitors traffic from and towards the client. As personal firewall sits in the device, which needs to be protected, it has access to additional client specific information in comparison to a gateway firewall. Therefore it is well suited for conducting functionality of the invention. However, the invention can be included also in some other application or equally it can be implemented on its own.

**[0034]** Figure 2A is a flow chart illustrating an example of the method of the invention. In step 200, a control connection originating from the client device, in which the method of the invention is used, is detected. Then in step 201, it is noticed that a related connection is negotiated within that control connection. As described above, negotiating a related connection comprises defining one of the ports of the client device for the related connection. In step 202, the relationship between the port negotiated for the related connection and the control connection is examined by checking, if the port was opened within a predefined time window in relation to noticing negotiation of the related connection. There are no restrictions for the duration of the time window, but a suitable value can be for example between 10 and 1000 seconds. If the port was opened within the time window, the related connection is allowed in step 204 and in the opposite case the related connection is blocked in step 203. This implementation clearly requires that for each open port of the device the moment of time when the port was opened needs to be recorded. This is

straightforward implementation detail for a man skilled in the art and thus not discussed any further herein.

**[0035]** Figure 2B is a flow chart illustrating another example of the method of the invention. Steps 200 and 201 are herein equal to respective steps in Figure 2A. But now the relationship between the port negotiated for the related connection and the control connection is examined by checking, if the same process family, which had opened the control connection, opened the port. In its simplest form process family may refer to only one process. In that case the method of the invention would simply check if the same process opened the control connection and the port. Another definition for a process family is that processes belong to the same family, if they have common parent process from which they are inherited. In that case the method of the invention would check if the process, which opened the control connection, and the process, which opened the port, have a common parent process. Still other possibility is that the method of the invention would check if the process, which opened the control connection, is a parent process for the process, which opened the port. Also some other relationship between processes may be regarded as an indicator of processes belonging to the same process family. Comparisons of the processes can be done e.g. by means of process ID (PID) values and parent process ID values (PPID). If the same process family opened the port, the related connection is allowed in step 204 and in the opposite case the related connection is blocked in step 203.

**[0036]** It needs to be understood that the network configuration of Figure 1 and the usage scenarios of the invention described above are only examples, and that the invention can be employed in various other ways within the scope of the invention.